SECTION I: DRAFT TRUST Program Information

The Defense Advanced Research Projects Agency (DARPA) often selects its research efforts through the Broad Agency Announcement (BAA) process. This request for information (RFI) is intended to provide details about a possible future DARPA program so that industry feedback can be considered prior to the issuance of a BAA. Responders are invited to provide comment on any or all of the content of this announcement to include suggestions for improving the scope of a possible solicitation in order to ensure that every effort is made to address this important problem. Responses to this request may or may not be incorporated within any future BAA announcement. In order to comply with scheduling priorities, responders are asked to provide feedback with 10 calendar days to jonathan.breedlove.ctr@darpa.mil.

DARPA is soliciting innovative research proposals to advance the science and technology for ensuring that integrated circuits can be trusted regardless of their origin and fabrication process. Proposed research should investigate innovative approaches that enable revolutionary advances in science, devices, or systems. Specifically excluded is research that primarily results in evolutionary improvements to the existing state of practice. Proposers are free to submit proposals on any or all of the specific interest areas specified in this announcement.

Background and Scope

Largely because of global economic pressures, fabrication of advanced integrated circuits is migrating to foreign foundries. In addition, business models are increasingly driven by commercial, rather then military, demand. Dedicated facilities (NSA, Sandia, Honeywell, etc.) cannot provide the performance, variety and volume of microchips that the DOD needs. These trends have raised concern regarding US weapons systems reliance on high performance microchips and potential vulnerabilities to these systems caused by malicious manipulation of hardware and software processes that might render these vital systems inoperable at some future time. This situation is true for both ASIC and COTS parts.

Furthermore there are issues with protecting intellectual property and military secrets as they are often embedded in the design of microcircuits, and the details of this design are often needed by the manufacturer in the fabrication process.

Finally there are also issues associated with protecting intellectual property and military secrets after the systems are deployed, especially in circumstances where systems and components are lost, captured or are no longer under US control and subject to reverse engineering over a sustained period of time.

This new DARPA initiative is being considered to address the above issues and others that have been identified in the DSB study on High Performance Microchip Supply [http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf]. The report addresses design, the use of advanced design tools, fabrication, packaging, testing, and monitoring of high performance IC's within critical systems and subsystems. As shown in Figure 1, specific areas of interest to DARPA include TRUST, Information Leakage and Anti-Tamper; although the primary interest is TRUST. DARPA will also engage in a Metrics-for-TRUST task focused on measuring the value of DARPA investments in novel technologies. To be clear, DARPA is only interested in issues related to TRUSTed Integrated Circuits and is not interested in proposals pertaining to issues concerning printed circuit boards or the general area of malicious software.

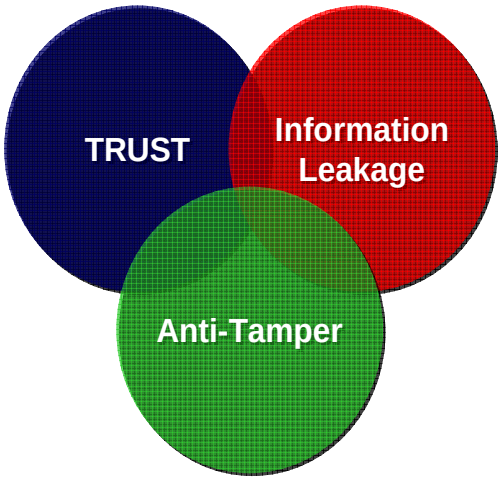

Figure 1 Overlap of Interests

The general areas of interest will identify and address potential vulnerabilities and will quantify the mitigation of these vulnerabilities through techniques and metrics-based evaluation. These areas include:

- TRUST for Integrated Circuits (IC's) – which will address the fundamental problem of determining if a microchip that is manufactured through a process that is inherently "untrusted" (i.e. not under our control) can be "trusted" to perform operations only as specified by the design, and no more,

- TRUST Against Information Leakage – which will address the fundamental problem of protecting intellectual property and design details from physical reverse engineering or other passive and active interrogation techniques,

- TRUST Against Tamper – which will address on-chip methods that can detect tampering and automatically take actions to protect intellectual property and

design details to include self destruct mechanisms if necessary and how to communicate the detection of tampering,

- Metrics for TRUST – which will devise quantitative measurements and testing procedures that can be used to compare alternative technologies for achieving TRUST in the above three areas.

It should be noted that the primary thrust of this effort is focused on TRUST for IC's. Proposers are free to submit proposals on any or all of the specific interest areas above.

Trustworthiness of microchips used in the DOD and the Intelligence Community has been a longstanding and recognized issue, even before the migration of fabrication processes to foreign foundries became so prevalent. The DOD "Trusted Foundry Program" which regulates and maintains a US-owned and operated fabrication facility was created to address these concerns. However, as highlighted in the DSB report referenced above, that the Trusted Foundry Program is viewed as a partial solution to a problem of growing concern. While the "Trusted Foundry Program" is viewed as an important and useful program, the DARPA TRUST Program is intended to develop technologies that can provide trust in the absence of a "trusted foundry". This DARPA effort is not intended to supplant the Trusted Foundry Program or improve its processes or capability. Rather, only technical efforts that address non-trusted foundries or COTS products will be considered.

Definition of the Adversary

DARPA is only interested in technologies that address TRUST issues created by a technically sophisticated, patient and fiscally well- endowed threat. It is assumed that the adversary is a Nation/State with modern semiconductor capability that has the:

- Motivation
- Opportunity
- Equipment
- Talent
- Manpower
- Time/Patience

to do significant harm to the US. It is also assumed that the adversary has the same or better offensive technology than the US.

Microchip Supply Chain Issues

The old supply chain model for integrated circuit design and fabrication is presented in Figure 2. In the past, when all of these processes were conducted in

the US, there was an opportunity to impart trusted control over all the design and fabrication steps.

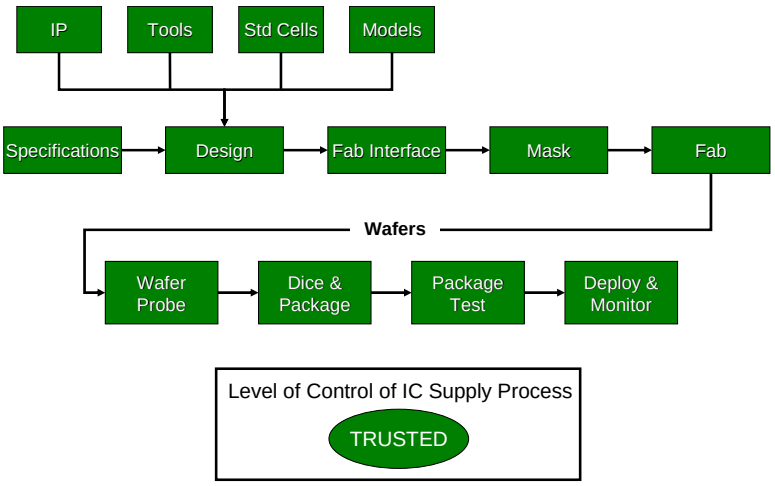

Figure 2 Old Supply Chain Structure

The evolving trend toward more offshore foundry fabrication has reduced the opportunity for controlling the process, rendering many of the process steps inherently untrustworthy. The new supply chain model is shown in Figure 3.

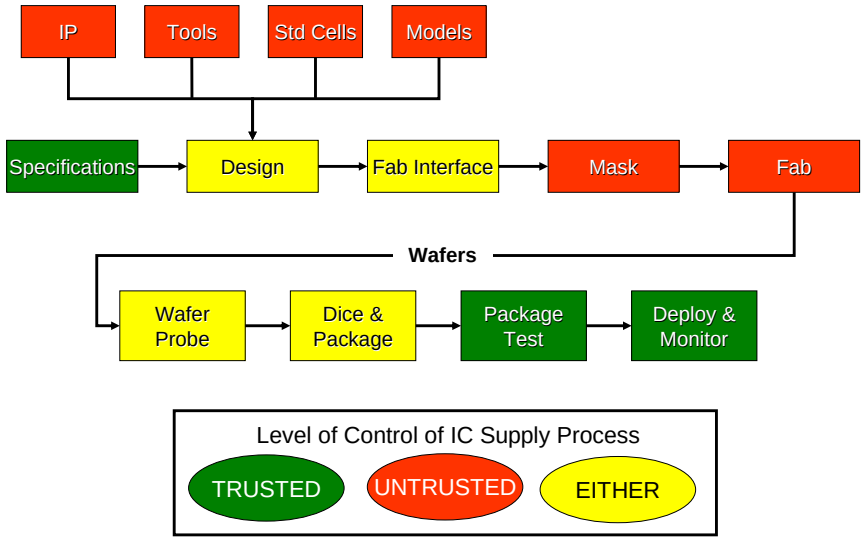

Figure 3 New Supply Chain Structure

There are several places in the design and fabrication process that are vulnerable in a variety of ways. One significant vulnerability is in the design. Some of the factors related to design that contribute are:

- There is a close coupling between fabrication and design, and as IC fabrication moves offshore, design is following it

- There are many opportunities for the introduction of unwanted features into the integrated circuit during the design cycle
- The design tools may also generate the functional test vectors used during packaged integrated circuit tests
- Many design tools are produced offshore
- Traditional "US" design tool vendors now do significant development work offshore

Several other elements of the foundry manufacturing process contain varying levels of vulnerability. For example, foundries may not accept photomasks that are not produced either internally or from their recognized supplier. Some foundries may allow independent wafer tests before packaging, while others may not. Dies may be distributed without packaging, may require packaging in-house, or may be sent to a third party provider as a final assembly step.
To fully assess the TRUST of a microchip, it is therefore fundamentally important to understand the vulnerabilities in all of the steps in the manufacturing process. Only then can these vulnerabilities be understood and addressed with techniques that mitigate them individually, as well as in an integrated end-to-end sense.

ASIC and COTS Vulnerabilities

Examination of the IC content of modern US weapons systems reveals that over 50 percent of the IC's are COTS parts, primarily FPGAs, rather then ASICs. Furthermore the majority of both COTS and the ASIC devices are produced overseas.

There are considerations regarding TRUST issues for ASIC designs that are different from issues associated with COTS designs. As shown in Figure 4, ASIC and COTS parts take different paths through the supply chain process. ASIC product consumers have more involvement in the entire process than COTS consumers. There is more control over the design process of an ASIC, but there is increased vulnerability from un-trusted design tools and a lack of control during the fabrication process. Since relatively small volume ASIC parts designed specifically for US military use may be easily recognized, they may be vulnerable to malicious circuit modifications or theft of design information. However, ASIC parts can allow more control over the wafer probing and packaging options.

It might be assumed that COTS products offer the advantage of being less of a target to an adversary; since the ultimate use of COTS products is more easily disguised (hidden in the weeds). This assumes however that correct supply chain management is employed and that there is no insider threat. It is therefore important to make sure that a substitution COTS part is not inserted into the supply chain. Furthermore; COTS parts have the likelihood of having hidden/private features which could be exploited, including malicious reprogramming. Testing for COTS TRUST is therefore a very difficult issue.

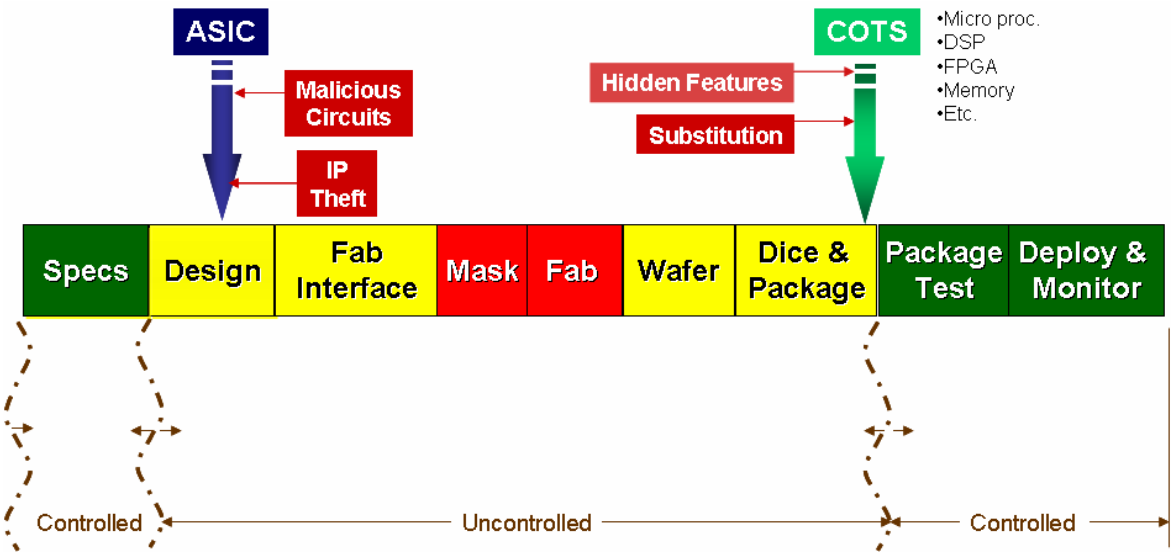

Figure 4 – Chip Development Process and Vulnerability

Also illustrated in Figure 4 is the fact that the process elements may or may not be in the control of the US microchip designer. Thus the control boundaries are not fixed, but rather depend on the design facility, the foundry, and the package supplier. These boundaries are not important for COTS products but are important for ASIC TRUST issues.

Technical Problems of Interest to DARPA

DARPA is interested in receiving proposals which focus only on techniques that ensure trust, along with measurements which quantify the improvement in trust. These measurements must be part of a metric associated with trust. It is required that each proposer have documented experience in IC technology (design, fabrication, testing).

Interested proposers are asked to submit technical ideas that address only the most difficult TRUST related issues. Examples of the type of problems that DARPA would like to address include:

- How do you trust the design cycle to faithfully generate only the microelectronics desired?
- How do you know that the Intellectual Property (IP) that you use in a design can be trusted?
- How do you trust microelectronics chips when they are manufactured in a non-trusted facility, such that they will faithfully and consistently perform only the functions they are designed for?

- How do you trust that the testing on the microelectronic chips will faithfully determine that the chip will operate over its lifetime only as designed? (no more – no less)
- How do you know that chip packaging does not introduce features into, or misidentify, the chip?
- How do you determine that the packaged chip has not been tampered with after installation, and how do you communicate the fact of tampering?

DARPA is interested in having a set of techniques which will ensure trust for the entire process flow that is shown in Figure 3. We do not expect that a single technique will allow protection across the entire process flow. Therefore DARPA will select techniques which allow the entire process flow to be protected. Each proposal should define if the technique is applicable to the ASIC case or to the COTS case or to both. The existence or creation of a "gold standard" may allow different techniques to be proposed. (i.e. we may have at least one chip of known trusted design in our possession)

The assumptions underlying each proposed technique must be clearly stated. In this regard, the following questions must be answered:

- What elements(s)/process step(s) of the process flow does the technique pertain to?
- What are the trusted/untrusted boundaries?
- What is the insertion point of the technique?
- What are the measurement points to determine the effectiveness of the technique?
- Is a gold standard assumed?

DARPA is not interested in proposals that focus on improving the reliability of IC's. Furthermore, while DARPA recognizes the merit of proper procedures to protect the design and fabrication of integrated circuits, DARPA is **not interested** in receiving proposals which are based on procedures (e.g. having a trusted design facility, having a trusted foundry, clearing all persons involved with the design and fabrication of the IC's, locking up data, etc).

Metrics

The development of useful metrics is itself viewed as a technical goal of the program as it is often difficult to develop these with sufficient detail to enable quantitative comparison of alternative technology investments. All technical proposals must contain clearly defined and testable metrics enabling technical progress to be measured and go/no-go decisions for continuing the program to be made. Independent of the technical performers who will define metrics to be used for evaluating their respective technologies, DARPA envisions the establishment metrics teams to support the agency in evaluating the scope and quality of metrics that are used and in conducting or overseeing tests that measure technical performance of the efforts. This

metrics and independent evaluation efforts will be the fourth thrust of the program and DARPA is interested in receiving proposals from organizations wishing to support this thrust.

The metrics effort will contain two thrusts: 1) Metrics Performers - focused on working with the technical performers for the refinement and continued development of individual and integrated system metrics that will be used to quantify performance improvement provided by the proposed technical efforts, and 2) Metrics Evaluators - focused on evaluating the value of the metric definition, parameters, and go/no-go thresholds proposed by the Metrics Performers. Figure 5 presents these two thrusts. The performance desired against metrics proposed can be represented graphically as shown.

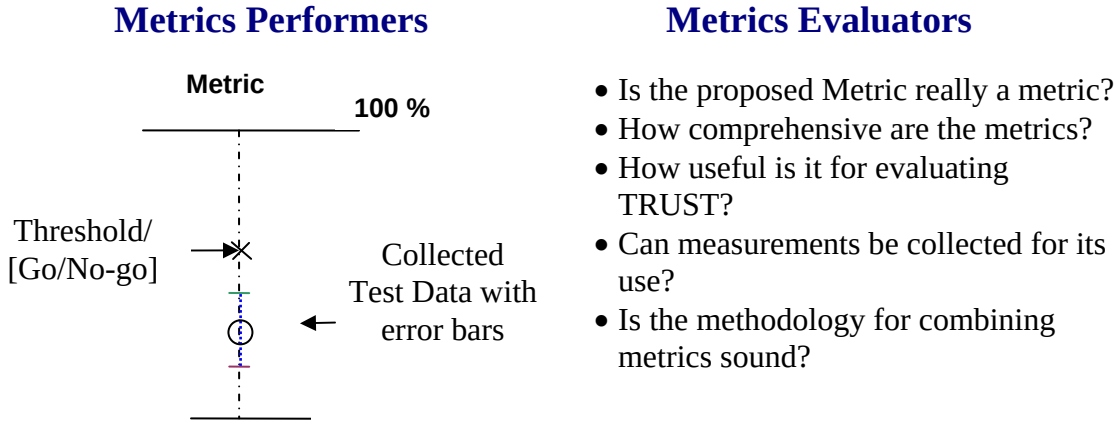

Figure 5 – Metrics Thrust Areas

DARPA envisions that the metrics teams will work with the technology provider teams in an integrated manner ensuring that each of the technology efforts clearly addresses a comprehensive evaluation plan at the outset of each effort.

Anticipated Program Plan

To meet program objectives, the TRUST for Integrated Circuits program is expected to have three phases.

- Phase I (18 Months) will focus on the identification and development of concepts and technologies that can prove feasible for developing trust, protecting intellectual property, and protecting against tamper. Technical efforts in each of the above areas are envisioned. A parallel Metrics initiative will be funded to provide the quantitative measures and testing procedures required to evaluate benefit from this feasibility phase.

- Phase II (18 Months) will focus on the further specific development of unique technologies identified in Phase I that will ensure TRUST, and protect against

Information Leakage and Tamper. Phase II will initiate system design, integration tasks and develop a testing process for extracting measurements that can be used for metrics-based evaluations. A parallel metrics effort will guide selection of specific projects in this phase.

- Phase III (18 Months) will involve prototype development of microchip integrated circuits that will be subjected to red team/black team evaluation and destructive reverse engineering to demonstrate TRUST in operation and protection against unwanted Information Leakage and Tamper. The Phase III effort will culminate in the successful development of a TRUSTed microchip using "untrusted" fabrication processes. A parallel metrics effort will guide selection of specific projects in this phase.

These periods of performance are approximate. Offerors who can meet the program goals on an accelerated schedule are highly encouraged to do so. Every proposer must include in their proposal a set of go/no- go milestones which must be met before the next program phase can be initiated. These milestones must be part of the TRUST metrics efforts.
Clearly stated, quantitative milestones are required for each of these Phases. Additional interim milestones at 6 month intervals are also highly encouraged. Organizations wishing to participate in Phase II or Phase III should include them as options in their proposals.

Specific Areas of Interest

I. Technologies for TRUSTed Integrated Circuits

Of paramount importance is a requirement that IC's developed, integrated and deployed contain only the circuitry, functional logic and support infrastructure that is specified without regard to where the chip is designed or fabricated.

In considering the microchip fabrication process it is important to consider all aspects of the design, manufacturing and deployment pipeline as depicted in Figure 3. As shown, this pipeline spans the entire life of the product from its initial design documentation/specification, through fabrication and delivery at the end of the supply chain, and through its useful life while deployed. For ASIC's, pipeline considerations include, but are not limited to, the following process steps:

- The use of design tools
- The creation of a Netlist and GDS II files
- The creation of photomasks
- Device fabrication
- Inspection and wafer testing
- Inspection and testing of individual chips cut from the wafer,
- Wire bonding or flip chip carrier attachment
- Packaging and product branding
- Testing of the packaged chip

- Monitoring the performance of the chip while deployed.

The requirement for TRUST applies to all IC's regardless of source (untrusted foundry or 3rd party vendor), quantity (large or small lots) or chip class (ASIC and COTS). The proposed efforts should fully address, at minimum, the following questions:

- Given an IC corresponding to a known design, does the IC that is delivered do what it is supposed to do and nothing more?
- Given an IC of unknown design, what does the IC do?

The worst case ASIC problem that we are trying to solve is the scenario where the customer provides input to a service provider(s) [assume service provider(s) are non-U.S.] in the form of a specification in some computer readable format (e.g., a Hardware Description Language (HDL)), and then receives a packaged chip back from a service provider (e.g., foundry). (Note: there may be multiple service providers involved in various phases of the process.) For a slightly less worse case scenario, it could be assumed that after providing the input specifications in HDL format to the service providers, the customer receives unpackaged wafers. Perhaps the best possible case would be where GDSII input was provided to the foundry and unpackaged wafers were received back from the foundry. Of course, in the case of a COTS part, one normally only receives the packaged device.

Technologies of interest include, but are not limited to:

- Detection of extra circuitry inserted in the design phase;
- Determination of the functionality of any extra circuits detected;
- Techniques to reduce the likelihood of additional circuits being inserted;
- Techniques which ensure that no additional circuitry beyond that specified in the design can be added to the chip layout during the fabrication process;
- Validation that test procedures for packaged chips are correct and comprehensive for only those aspects of functionality specified in the design;
- Allowing comparison of one packaged integrated circuit to another packaged integrated circuit, to determine if both devices are identical;
- Determination of the state of hidden/private functions in COTS parts.

Proposers must include a clearly defined set of metrics and methods for testing and evaluating the performance of their technical efforts against a defined baseline. All approaches and program plans must include milestones with go/no-go milestones every 6 months.

II. TRUST Against Information Leakage

There is concern that techniques can be used to extract information directly from an integrated circuit, passively or actively, as an individual component, and/or as a deployed element of an integrated system. Circuit function details may also be

obtained during the design stage. Information to be protected includes the intellectual property associated with a chipset and its design, data associated with both the hardware and deployed software, and data embedded or downloaded to the integrated circuit either prior to or during operation. Examples of information attacks on integrated circuits include side-channel attacks to extract certain key material, and destructive and nondestructive reverse engineering that can reveal the circuitry associated with the original design. The latter attacks, in addition to exposing data that should be protected, often provide enough information to allow counterfeit manufacture thereby further confounding chip pedigree determination for some verification processes.

Technologies of interest in this area include, but are not limited to, those that eliminate the ability to:

- Gain information about the design of an integrated circuit or data contained therein from active probes, supply voltage/current monitoring, test vector manipulation or other approaches;
- Conduct passive detection of electromagnetic, thermal or other phenomena that may convey information about the inner workings or design of the integrated circuit or its associated data;
- Conduct active inspection of the physical microchip to include destructive testing that expose circuits thereby enabling the characterization of the underlying design;
- Conduct unauthorized transmission of on-chip data through exploitation of the data bus or other connections required for the normal operation of the microchip.

Proposers must include a clearly defined set of metrics and methods for testing and evaluating the performance of their technical efforts against a defined baseline. All approaches and program plans must include milestones with go/no-go milestones every 6 months.

III. TRUST Against Tamper

Protection against future tampering of IC's once they are deployed in operation, independently or as part of an integrated subsystem, is a concern. For military applications, IC's are also vulnerable to tampering in those situations where weapon system parts or entire platforms are sold to second parties, acquired accidentally, or through other compromise situations. In these events, it is important that methods be in place to protect integrated circuits designs and data against prolonged inspection and tampering that might reveal the function and data associated with an IC. A broad interpretation of tampering activities should be taken to include destructive methods that involve physical activities and non-destructive methods. These methods may include altering the IC environment (EM, thermal, or other) to spoof sensors and on-chip protection to conclude that it is operating in a safe environment and thus can function as designed.

DARPA is only interested in anti-tamper efforts at the packaged IC level, and not at the system level.

Technologies of interest include, but are not limited to:

- Intelligent sensor packaging methods that render the payload useless when tampered with;
- On-chip micro-sensors and processing circuitry that can detect tampering activities and render the chipset useless while eradicating sensitive data;
- One-time packaging concepts that cause disintegration of an operating chip when physically probed;
- Circuits and on-chip sensors that can characterize its own chip operations (through EM, thermal, or other phenomena), detect deviations from normal operations, and render the chipset useless when deviations from normal operations are detected;
- Obfuscation techniques that hide data or circuit functionality regardless of success of tamper activities;
- Techniques to allow the IC to "call home" when it is attacked.

Proposers must include a clearly defined set of metrics and methods for testing and evaluating the performance of their technical efforts against a defined baseline. All approaches and program plans must include milestones with go/no-go milestones every 6 months.

IV. Metrics and Performance Evaluations of Technologies for TRUST

In addition to areas where technology must be developed, there is also a need to develop metrics and testing procedures so that the effectiveness of proposed technical solutions can be assessed and compared. This area of interest will explore methods to quantify and develop metrics with the goal of providing a "figure of merit" for assessing how particular technologies might improve trust in the development and utilization of IC's. As DARPA invests in alternative technologies to deliver enhanced "trust" in integrated circuits, it is important that these methods be tested in a manner that quantifies performance gain against some known current baseline. Therefore DARPA is interested in deriving and measuring baseline metrics performance of TRUST as well as deriving tests and experiments that can be used to measure progress and improvement as investments in technology programs are made.

DARPA envisions a metrics team that will work with the technical providers to provide a structured approach for refining metrics and conducting evaluations of alternative technical approaches. The fundamental steps of a metrics program involve the following steps:

- **Defining Metrics**

- Problem addressed
- Metric
- Metric definition
- Define go/no-go value and required coverage for the metric
- Tests based on the metric
- Define any dependencies that this measurement/test might have on other measurements/tests.

- **Applying and Evaluating Metrics:**
  - Conduct the test and collect test/measurement data on the property
  - Determine where the data fits within the metric scale [Go/No-Go]

Metrics Performers will work on defining metrics. Metrics Evaluators will work on applying and evaluating metrics.

Methods of interest include, but are not limited to:

- Derivation of quantitative methods for establishing the baseline TRUST worthiness of microchips when measured against the three major categories of TRUST for Integrated Circuits, TRUST Against Information Leakage, and TRUST against Tamper;
- Derivation of quantitative metrics to be applied to future design and fabrication processes;
- Experiments and tests that can be readily performed to assess the TRUSTworthiness of the design, fabrication, test and deployment processes;
- Compound metrics that incorporate quantitative individual technology metrics that can provide an overall assessment of TRUST that spans the entire design and manufacturing process.
- An experiment, test and evaluation process that can be used by DARPA to help assess, quantitatively, the improvement in TRUST provided by its technology development programs.

Proposed approaches should address;

- The measures to be evaluated, the assessment method or framework, the design of experiment approach, configuration, modeling, test data generation, test execution, data capture, analysis, and reporting mechanisms and automation already developed or proposed in any of the above;
- Requirements that will be placed for interfaces, instrumentation, protocols or formats;
- Non-interference of test instrumentation, portability, repeatability, cost-effectiveness, and organic or contracted expertise in creating effective test samples representing nation-state threat capabilities in the compromise of integrated circuit manufacture;
- Test sets employed that represent the range of threats and consequences;
- Test frameworks that can validate and verify different technologies introduced at various stages in the lifecycle of integrated circuits;

- Quantitative and experimental evaluation that is scientifically rigorous and repeatable is essential to be considered for award.
- Securing the test procedure specifications, results, and analyses.

Quantitative and experimental evaluation that is scientifically rigorous and repeatable is essential to be considered for award. It is envisioned that technical performers of this task will become involved in the testing and evaluation of the other three technology development areas of the DARPA TRUST Program. Therefore, although not required, it is reasonable to expect that technical performers in this area will not be the same as those providing technologies for TRUSTed Integrated Circuits, prevention of Information Leakage and protection against Tamper. If the proposer of this effort wishes to also propose in any of the other three areas, a work scope "firewall" must be defined to DARPA's satisfaction.

Program Milestones

As was discussed earlier, each of the elements of the "new" supply chain process present varying levels of TRUST vulnerability. Therefore it will be important to establish metrics that can be used to assess the improvement in TRUST or reduction in vulnerability as a result of a given technology from the perspective of a specific IC manufacturing process step. In addition it is important that overall metrics be established that can quantify performance improvement over the entire end-to-end supply chain.

Comprehensive/allover metrics can be of three complementary types:

Type a: Increasing the difficulty of an adversary to overcome the TRUST techniques employed
Type b: Increasing the ease in detecting an adversary's actions
Type c: Engineering costs associated with implementing TRUST techniques

The following items are viewed as candidate overall metrics for the program:

- **Type a:**
  - Time to defeat TRUST measures
  - Manpower and skill level to defeat TRUST measures
  - Cost of equipment to defeat TRUST measures

- **Type b:**
  - Reduction of time needed to detect malicious circuits in ASIC's.
  - Reduction of manpower and skill level needed to detect malicious circuits in ASIC's.
  - Reduction of cost of equipment needed to detect malicious circuits in ASIC's.

- Reduction of time needed to detect a substituted ASIC or COTS part.
- Reduction of manpower and skill level needed to detect a substituted ASIC or COTS part.
- Reduction of cost of equipment needed to detect a substituted ASIC or COTS part.

- Reduction of time needed to determine the state of hidden/private information in COTS parts.
- Reduction of manpower and skill level needed to determine the state of hidden/private information in COTS parts.
- Reduction of cost of equipment to determine the state of hidden/private information in COTS parts.

- **Type c:** Every proposed Trust technical approach must quantify the effect of their technique on:

  - Length of Design time
  - Performance (speed)
  - Power
  - Fabrication cycle time
  - Chip size
  - Reliability
  - Circuits types impacted (e.g. FPGA)
  - Cost

Candidate critical milestones for the program by phase are:

- Phase I milestone of 10X improvement over a defined baseline state-of-the-art
- Phase II milestone of 100X improvement
- Phase III milestone of 1000X improvement

In the proposals, the state-of-the-art baseline value for the above items must be stated. In addition, a method must be proposed to combine the various types above to demonstrate the 10/100/1000 X improvements.